PATENTS • DESIGNS • The Patent Office • COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

#3

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

CERTIFIED COPY OF PRIORITY DOCUMENT

Signed JEvans.

Dated 12 March 2001

BLANK PAGE

Patents Form 7/77

Patents Act 1977
(Rule 15)

7/77

Statement of inventorship and of right to grant of a patent

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference
P/23726.GB/CJW

2. Patent application number *(if you know it)*
0016553.0 05 JUL 2000

3. Full name of the or of each applicant
GFI FAX & VOICE LTD.

4. Title of the invention
ELECTRONIC MAIL MESSAGE ANTI-VIRUS SYSTEM AND METHOD

5. State how the applicant*(s)* derived the right from the inventor*(s)* to be granted a patent
BY CONTRACT OF EMPLOYMENT

6. How many, if any, additional Patents Forms 7/77 are attached to this form?
(see note (c))
--

7. I/We believe that the person*(s)* named over the page *(and on any extra copies of this form)* is/are the inventor*(s)* of the invention which the above patent application relates to.

Signature Langner Parry
LANGNER PARRY

Date 5 July 2000

8. Name and daytime telephone number of person to contact in the United Kingdom
CLIFFORD J WANT 020 7242 5566

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500 505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.

d) When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.

e) Once you have filled in the form you must remember to sign and date it.

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

NICK GALEA

"MARATEA"
ENRICO NAUDI STREET
IKLIN
MALTA

Patents ADP number *(if you know it)*: 7934771001

Patents ADP number *(if you know it)*:

Reminder

Have you signed the form?

Patents ADP number *(if you know it)*:

Patents Form 1/77

Patents Act 1977
(Rule 16)

1/77

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1. Your reference

P/23726.GB/CJW

2. Patent application number
(The Patent Office will fill in this part)

0016553.0

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

GFI FAX & VOICE LTD
PO BOX 362
ROAD TOWN
TORTOLA
BRITISH VIRGIN ISLANDS

Patents ADP number *(if you know it)*

7934763001

If the applicant is a corporate body, give the country/state of its incorporation

BRITISH VIRGIN ISLANDS

4. Title of the invention

ELECTRONIC MAIL MESSAGE ANTI-VIRUS SYSTEM AND METHOD

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

LANGNER PARRY
52-54 HIGH HOLBORN
LONDON
WC1V 6RR

Patents ADP number *(if you know it)*

1032001 ✓

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

BLANK PAGE

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description 10 /

Claim(s) to follow

Abstract to follow Q

Drawing(s) 6 +6 ✓

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent *(Patents Form 7/77)* 1 / A

Request for preliminary examination and search *(Patents Form 9/77)*

Request for substantive examination *(Patents Form 10/77)*

Any other documents *(please specify)*

11. I/We request the grant of a patent on the basis of this application.

Signature Langner Parry
LANGNER PARRY

Date 5.7.00

12. Name and daytime telephone number of person to contact in the United Kingdom CLIFFORD J WANT 020 7242 5566

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

BLANK PAGE

ELECTRONIC MAIL MESSAGE ANTI-VIRUS SYSTEM AND METHOD

This invention relates to an electronic mail message anti-virus system and method.

Computers and computer networks are susceptible to attack from an HTML electronic mail message that contains a malicious code or the ability to trigger a program that could damage the computer system upon receipt of the electronic mail message. Anti-virus systems have been developed to detect such viruses which would otherwise infect a computer. Versions of anti-virus systems are known for detecting viruses transmitted by electronic mail. However, known anti-virus systems have been largely unsuccessful in combating viruses delivered by electronic mail for a number of reasons. First, known systems can only protect against known viruses. This may be done by scanning an incoming electronic mail message for strings of characters which are known to be included in known viruses. However, because such systems can only protect against known viruses and since electronic mail can spread viruses in a matter of hours, such systems are completely ineffective against electronic mail viruses as the anti-virus system cannot be updated with strings associated with the new virus before the computer is infected. Another problem with conventional electronic mail virus detection is that not all viruses are widespread. A virus may be created against a particular company, to obtain particular information from that company, for example, for industrial espionage. In that case, no measures can be taken to protect the system from the virus because the virus is not known until after the attack has occurred. Another problem with conventional anti-virus systems is that they scan only the attachment of an electronic mail message and not the electronic mail body itself. However, electronic mail viruses may not only be contained in attachments but may be contained in the message body itself, in which case, a virus can be activated without the user opening an electronic mail attachment.

It is an object of the present invention to provide an anti-virus system and method which substantially overcome these limitations.

According to the present invention there is provided an anti-virus system for an electronic mail message, the system including means for determining the presence of the electronic mail message; means for analysing and scanning the electronic mail message for tags indicating the presence of operable program code and for removing any such tags and operable program code from the electronic mail message; and means for applying the electronic mail message with the tags and operable program code removed to server means.

Preferably, the means for determining the presence of the electronic mail message includes means for breaking the message into constituent bodies or message texts and attachments of the electronic message; the means for analysing and scanning comprises means for scanning the constituent bodies and attachments and the means for applying the electronic mail message with the tags and operable program code removed to server means includes means for rebuilding the electronic message from the constituent bodies and attachments.

Conveniently, the means for analysing and scanning comprises means for scanning the message for predetermined character strings.

Advantageously, the means for applying the electronic mail message with the tags and operable program code removed to server means includes means for replacing the removed tag and operable program code with alternative text.

Preferably the alternative text is adapted to inform a recipient of the message that operable program code has been removed.

Advantageously the means for analysing and scanning includes means for scanning attachments for operable macros.

Advantageously the system further comprises quarantine means for quarantining a constituent body containing operable program code and/or removing from the message and quarantining an attachment containing a macro.

Preferably the quarantine means includes means for removing a macro from an attachment, quarantining the macro and releasing the attachment with the macro removed.

Preferably the quarantine means includes means for storing the body, attachment or macro in a quarantine storage location as a quarantined item; means for receiving a input indicating a decision whether the quarantined item may be delivered to an intended recipient; and dependant on the decision input either releasing the quarantined item for delivery to the intended recipient or deleting the quarantined item.

Conveniently, the quarantine means includes means, on deleting the quarantined item, for informing the intended recipient and/or a sender of the message that the quarantined item has been deleted without being delivered to the intended recipient.

Conveniently the means for scanning attachments for operable macros comprises means for sequentially scanning the attachments for a plurality of predetermined character strings.

Preferably, the means for scanning attachments for a plurality of predetermined character strings includes means for terminating scanning when one of the predetermined strings is not found on completely scanning the attachment.

Conveniently, the means for determining the presence of the electronic mail message is adapted to capture all electronic mail messages passing between a first network and a second network.

Advantageously, the means for determining the presence of the electronic mail message is adapted to capture all electronic mail messages passing between an internal or private network and an external or public network.

According to a second aspect of the present invention there is provided a method of removing a virus from an electronic mail message including the steps of (a) capturing the message; (b) scanning the message for tags indicating the presence of operable program code; (c) removing the tags and operable program code from the electronic mail message; and (d) releasing the electronic mail message with the tags and operable program code removed.

Alternatively, step (c) comprises quarantining a message or a part of a message containing operable program code.

Preferably step (a) includes the step of breaking the message into constituent bodies or message texts and attachments of the electronic message; step (b) comprises scanning the constituent bodies and attachments and step (d) includes the step of rebuilding the electronic message from the constituent bodies and attachments.

Conveniently step (b) comprises scanning the message for predetermined character strings.

Advantageously step (c) includes replacing the removed tag and operable program code with alternative text.

Preferably the alternative text is adapted to inform a recipient of the message that operable program code has been removed.

Advantageously step (b) includes scanning attachments for operable macros and step (c) comprises removing from the message and quarantining any macros or, alternatively, any attachments containing macros.

Preferably the step of quarantining a constituent body, attachment or macro comprises the steps of: storing the constituent body, attachment or macro in a quarantine storage location as a quarantined item; receiving a decision whether the quarantined item may be delivered to an intended recipient; and dependant on the decision either releasing the quarantined item for delivery to the intended recipient or deleting the quarantined item.

Conveniently, the step of deleting the quarantined item includes informing the intended recipient and/or a sender of the message that the quarantined item has been deleted without being delivered to the intended recipient.

Conveniently the step of scanning attachments for operable macros includes sequentially scanning the attachments for a plurality of predetermined character strings.

Preferably, the step of scanning attachments for a plurality of predetermined character strings is terminated when one of the predetermined strings is not found on completely scanning the attachment.

Conveniently, step (a) comprises capturing all electronic mail messages passing between a first network and a second network.

Advantageously, step (a) comprises capturing all electronic mail messages passing between an internal or private network and an external or public network.

According to a third aspect of the invention, there is provided a computer program comprising code means for performing all the steps of the method described above when the program is run on one or more computers.

Conveniently the computer program is embodied on a computer-readable medium.

According to a fourth aspect of the present invention, there is provided a computer program product comprising program code means stored in a computer-readable medium for performing the method described above when that program product is run on one or more computers.

An advantage of the present invention is that it does not seek to determine whether program coding included with an electronic message is malicious or not, but removes the capability of such an electronic mail message to execute the program or commands. That is, all electronic mail messages scanned that contain program code or instructions to run programs, are re-written in such a way that this capability is removed from the electronic mail message, or the message or part of the message containing the operable code is quarantined. This secures the recipient against all current, future and one-off viruses.

A specific embodiment of the invention will now be described by of example, with reference to accompanying drawings, in which:

FIG 1 shows a flowchart of a method, according to the present invention, of removing operable program code from a body or attachment of an electronic mail message;

FIG 2 shows a flowchart of a method according to the invention of removing macros or attachments which contain macros from an electronic mail message;

FIG 3 shows a flowchart of steps of the method of FIG 2 for determining whether an electronic mail message contains a Microsoft Word™ macro;

FIG 4 shows a flowchart of steps of the method of FIG 2 for determining whether an electronic mail message contains a Microsoft Excel™ macro;

FIG 5 shows a block diagram of building blocks used in the method of the invention;

FIG 6 shows the flow of electronic mail messages through a computer system employing the method of FIGS 1 & 2; and

FIG 7 shows steps in quarantining attachments of the method of FIG 2.

In the drawings, like numerals denote like steps.

FIG 1 illustrates an application of the invention in which the method of the invention is used in a gateway or electronic mail server, between a user's network and a public network, for example. However, it will be appreciated that the invention may be used to protect a single computer. As illustrated in FIG 1, an electronic message received by the electronic mail server, step 101, is isolated, or captured, step 102. The captured electronic mail message is divided up, step 103, into its constituent bodies of message text 110,111 and attachments 112,113. An electronic mail message can have multiple bodies, also known as message text, and multiple attachments, but only two of each are illustrated in FIG 1. The bodies and attachments are sequentially scanned, step 104, to determine whether any of the said bodies or attachments contains a character string indicating the presence of operable program code. That is, the program scans the body or attachment for a tag or tags which identify program code that will be run on viewing the electronic mail message or code that will run an external program executed once the electronic mail message is viewed. For example, in the current version of HTML the tag "scripts" identifies program code. The presence of such a tag means that an electronic mail message can potentially run an external program or trigger a program. It will be understood that for future or different versions of HTML, there may be more or different names for identifying script code. However, amending the method at step 104 to scan for such different character scripts is a trivial task compared with the impossibility of updating known anti-virus systems with character strings from all viruses in advance. If a script tag is found in an embodiment or attachment, the program is removed, step 105, from the body or attachment and preferably replaced with replacement text. Such replacement text may indicate to the eventual recipient of the electronic mail message that operable code has been removed. The electronic mail message is reassembled, step 106, by the electronic mail analyser program, that is, the electronic mail message is reconstituted from the separate bodies and the attachments reattached so the electronic mail message is recreated. The electronic mail message is passed, at step 107, back to the electronic mail server for forwarding, step 108, to the intended recipient. The intended recipient, therefore, receives a cleaned electronic mail message, which has no capability of running any programs and is, therefore, completely secure. Alternatively, the message containing script tag may be quarantined until subsequently released or deleted.

Simultaneously, or sequentially, the attachments are scanned to determine the presence of macros, as illustrated in FIG 2. As already described in relation to FIG 1, incoming or outgoing electronic mail messages are received by the electronic mail server, step 201, and an electronic mail message is isolated, step 202, and any attachments 212,213 are removed, step 203, from the electronic mail message and sequentially scanned to determine whether the attachments contain macros, step 214. If a macro is detected within an attachment, the attachment may either be deleted, step 215, or quarantined, step 216. Alternatively, the macro may be quarantined and the attachment released with the macro removed. If the macro or attachment is quarantined, a decision will subsequently be made, step 217, whether the macro or attachment should be deleted, or reassembled and reattached to the electronic mail message, step 218, or forwarded by other means to the intended recipient. If no macros are found in the attachment, then the attachment is reattached to the electronic mail message, step 218, and the electronic mail message is passed back to the electronic mail server, step 219, for forwarding, step 220, to the intended recipient. If an attachment has been deleted then a new attachment may be attached to the electronic mail message indicating to the intended recipient that the original attachment has been removed. In this manner, the method of the invention automatically removes any attachments from an electronic mail message which have the capability of running program codes or external programs by using macros. That is, all macros or attachments containing macros are removed and deleted, or at least quarantined, whether they are harmful or not.

As shown in FIG 3, if, for example, the analyser determines that an attachment is a Microsoft Word™ document, the attachment is searched sequentially for a number of character strings, thus the attachment is initially searched, step 301, for the character string "Root Entry". If the character string is not found, it is thereby determined that the attachment does not contain a macro and the attachment is released for rebuilding the message, step 218. If, however, the string is found, the attachment is rescanned, step 302, for string "VBA" and as in the previous step, if the string is not found, the attachment is released, otherwise the attachment is rescanned sequentially in the same manner for the string "PROJECT", step 303, and "DocumentSummaryInformation", step 304. If the attachment is found to contain all four of the strings, the attachment is either deleted, step 215, or quarantined, step 216.

Similarly, FIG 4 shows the procedure where the analysing program determines that the attachment is a Microsoft Excel™ document, in which the attachment is sequentially tested for the strings "Root Entry", "DocumentSummaryInformation", "Macros", "VBA" and "PROJECT", steps 401-405. Once again, if the attachment is found to contain all five of these strings, it is determined that the attachment contains a macro and the attachment is either deleted, step 215, or quarantined, step 216. Alternatively, just the macro may be detached and quarantined. It will be appreciated that if other known types of documents are detected they may be scanned in similar ways for appropriate character strings.

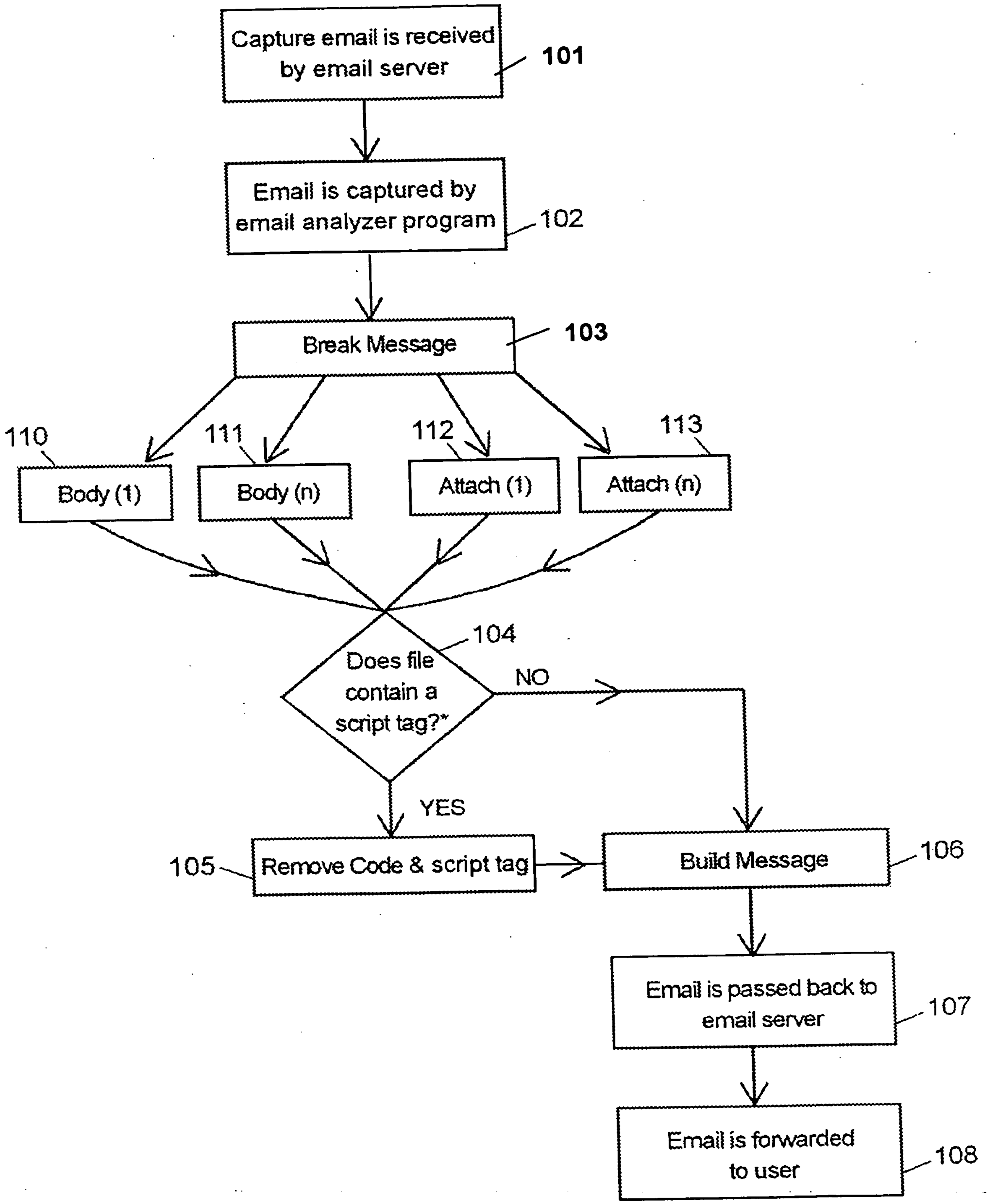
A block diagram of building blocks used in the method of the invention is shown in FIG 5. A capture and release server component 502 transports mail into and out of the analysing system. The server component interfaces with an external mailing system 501, such as Microsoft Exchange Server, Lotus Notes or SMT/POP 3 servers. This server component interface enables the electronic mail analyser to capture all incoming and outgoing mail and places incoming mail 503 and outgoing mail 504, in a process queue 505. An electronic mail analysing component 506 analyses electronic mail messages from the processing queue 505 sequentially. This electronic mail analysing component consists of a backbone which controls a number of smaller modules which perform specific actions on the electronic mail message, such as a module for breaking the message into parts 507, a module for searching for character strings or keywords 508 that identify program code and a module for checking attachments for macros 509. These so-called plug-in modules provide all the electronic mail processing intelligence to the system, and the backbone manages the message process queue. The electronic mail analyser therefore submits each of the electronic mail messages to the plug-ins in turn. In addition to those already described, there may be additional plug-ins for decrypting the message body as well as, for example, checking the message content. Once an electronic mail message has been processed by all the plug-ins, the electronic mail analyser returns the message to the capture and release server component which releases a virus-free message to the external mailing system for delivery to the intended recipient.

As shown in FIG 6, the electronic mail analysing component, 506, is a central part of the overall system and a capture and release server component 502, both passes electronic mail message from an external electronic mail system 501 to the electronic mail analysing component 506, and after processing, the server component 502 passes an electronic mail message 510 back to the electronic mail system.

In certain circumstances a user may, for example, wish to be able to receive electronic mail attachments containing macros from, for example, particular known users. It will be understood that user settings may be stored in the electronic mail analysing component, 506 to specify whether embedded HTML scripts and macros are to be removed from all electronic mail messages or whether exceptions are to be made for messages received from or sent to particular users. In such a situation, the system would first check whether user settings exist for the particular sender and recipient of a captured message and if so the user settings would be applied and if not, default settings would be used.

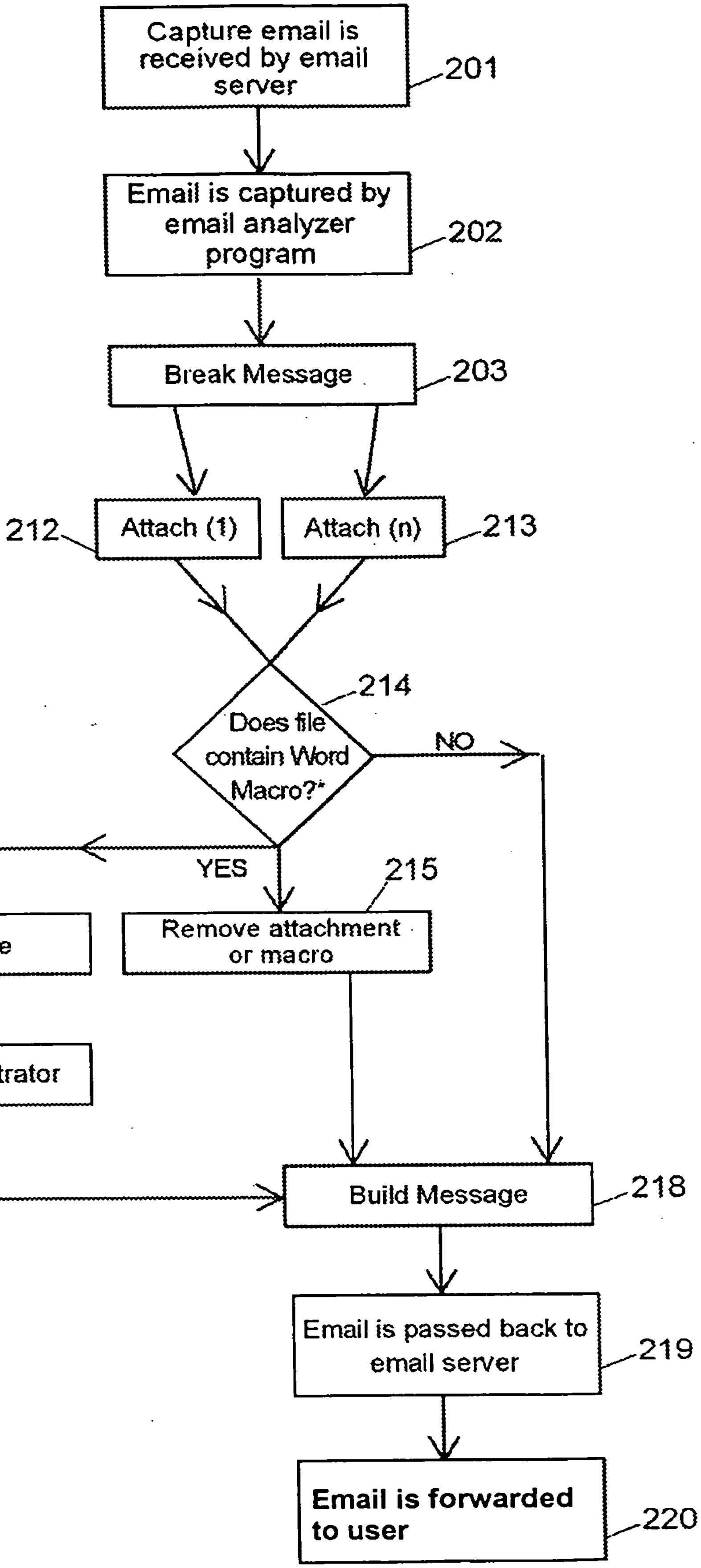
As best shown in FIG 7, an electronic mail message having program code, or attachments having program code or containing macros, is passed by a quarantine component 701 into quarantine 700. The quarantined message or message component is held while an authorised person is notified 702 to reject or approve the message, the authorised person being chosen from a list 703 of persons qualified to approve or reject quarantined mail. Dependent on the decision made, the quarantined message may be rejected, step 704, and deleted, step 705, in which case, optionally, the sender and/or recipient may be notified 706 that the message or message or component has been deleted. Alternatively, step 707, the quarantined message is approved and the message or component passed back to the server component, step 708, for delivery to the intended recipient.

Fig 1.


Capture email is received by email server
101
Email is captured by email analyzer program
102
Break Message
103
110
Body (1)
111
Body (n)
112
Attach (1)
113
Attach (n)
104
Does file contain a script tag?*
NO
YES
105
Remove Code & script tag
Build Message
106
Email is passed back to email server
107
Email is forwarded to user
108

BLANK PAGE

Fig 2.


Capture email is received by email server
201
Email is captured by email analyzer program
202
Break Message
203
212
Attach (1)
Attach (n)
213
214
Does file contain Word Macro?*
NO
YES
216
215
Quarantine
Remove attachment or macro
217
Inform Administrator
Build Message
218
Email is passed back to email server
219
Email is forwarded to user
220

BLANK PAGE

Fig 3.

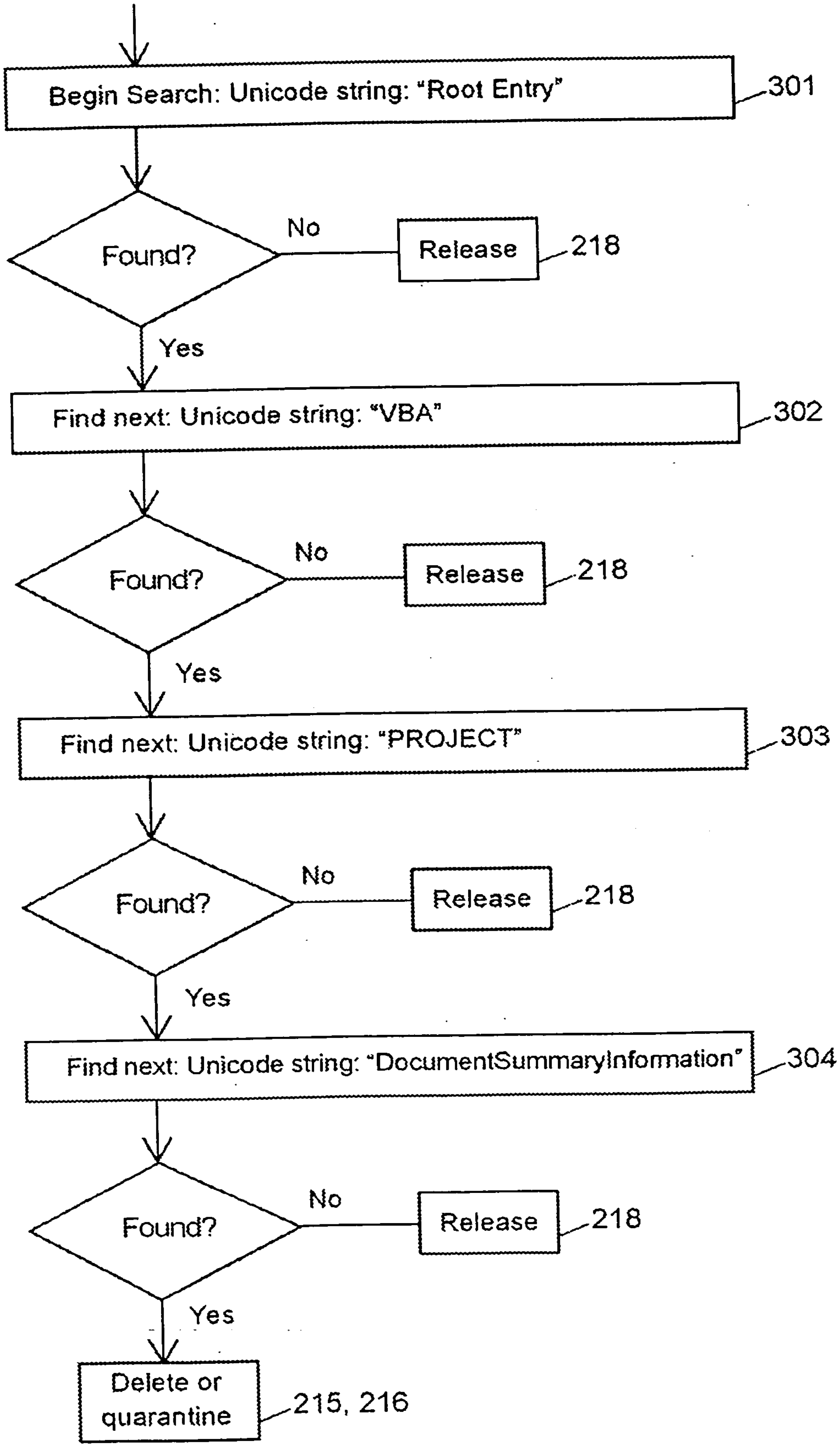
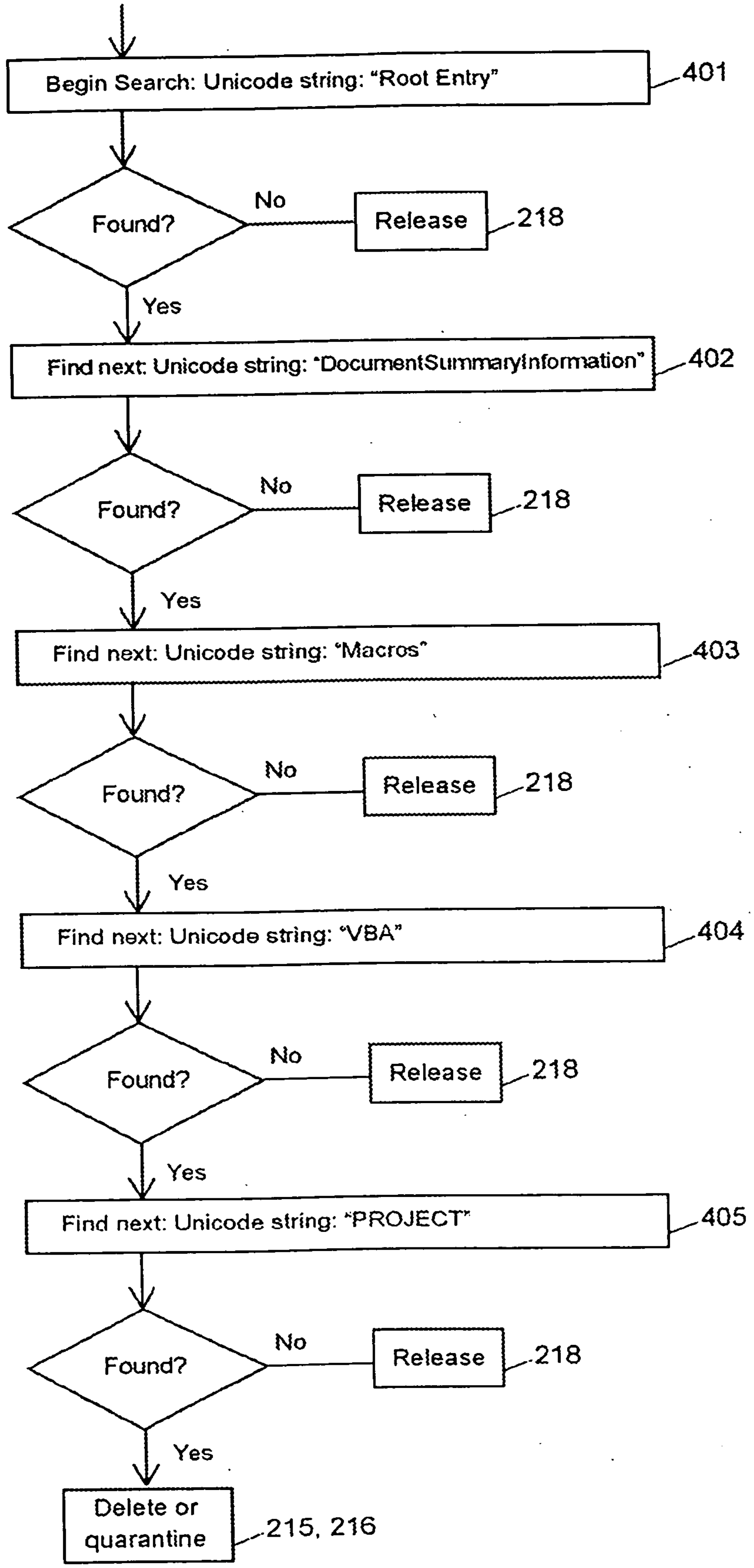

Begin Search: Unicode string: "Root Entry"
301
Found?
No
Release
218
Yes
Find next: Unicode string: "VBA"
302
Found?
No
Release
218
Yes
Find next: Unicode string: "PROJECT"
303
Found?
No
Release
218
Yes
Find next: Unicode string: "DocumentSummaryInformation"
304
Found?
No
Release
218
Yes
Delete or quarantine
215, 216

Fig 4.


Begin Search: Unicode string: "Root Entry"
401
Found?
No
Release
218
Yes
Find next: Unicode string: "DocumentSummaryInformation"
402
Found?
No
Release
218
Yes
Find next: Unicode string: "Macros"
403
Found?
No
Release
218
Yes
Find next: Unicode string: "VBA"
404
Found?
No
Release
218
Yes
Find next: Unicode string: "PROJECT"
405
Found?
No
Release
218
Yes
Delete or quarantine
215, 216

BLANK PAGE

Fig 5.

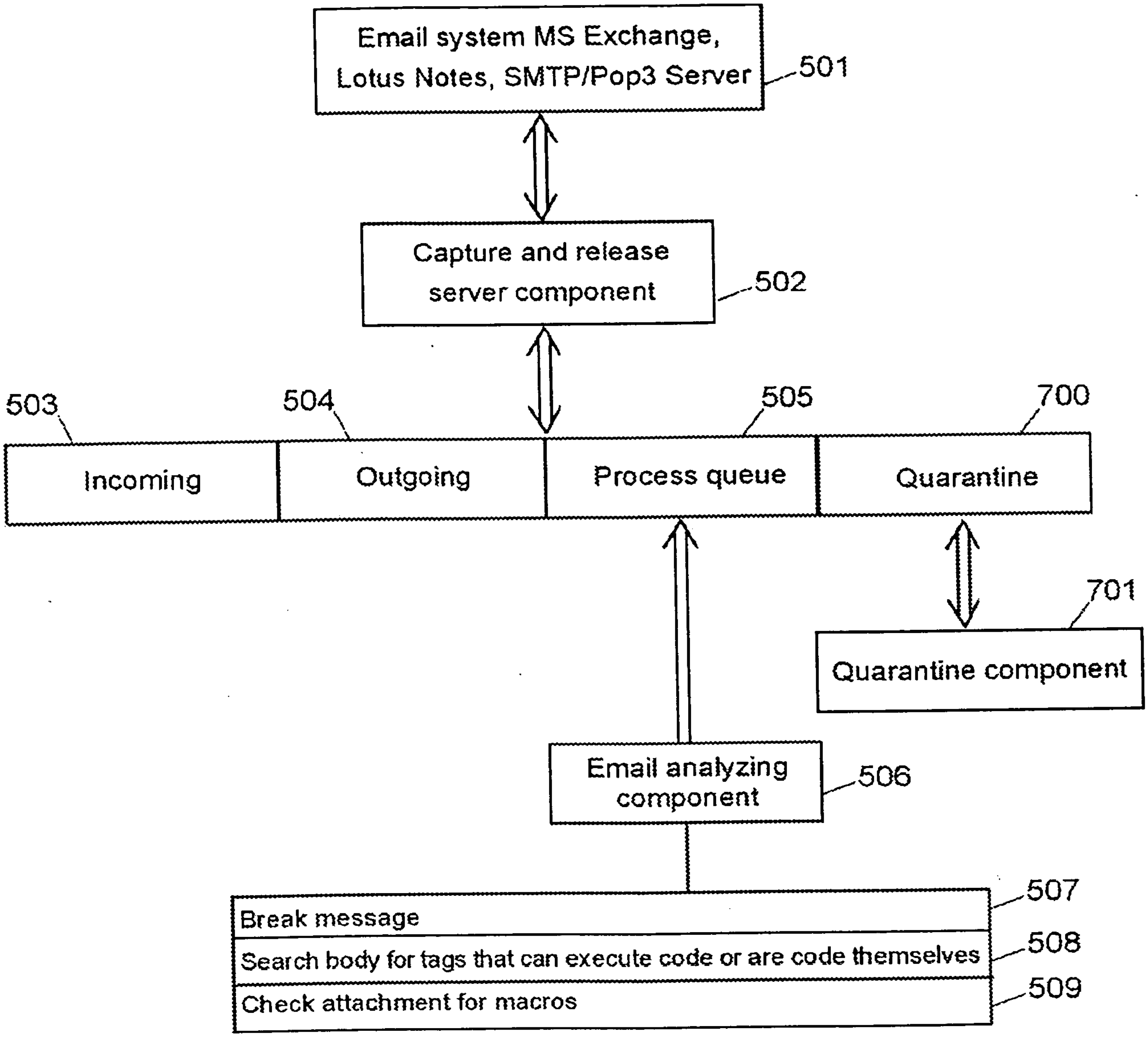

Email system MS Exchange, Lotus Notes, SMTP/Pop3 Server
501
Capture and release server component
502
503
504
505
700
Incoming
Outgoing
Process queue
Quarantine
701
Quarantine component
Email analyzing component
506
Break message
Search body for tags that can execute code or are code themselves
Check attachment for macros
507
508
509

Fig 6.

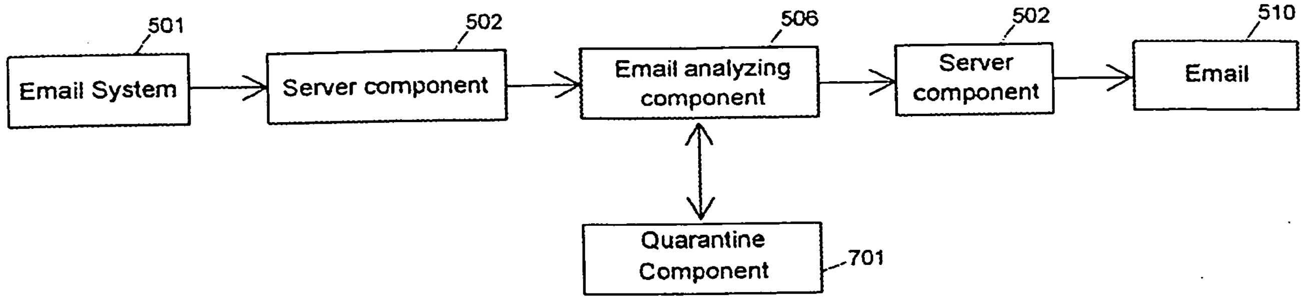
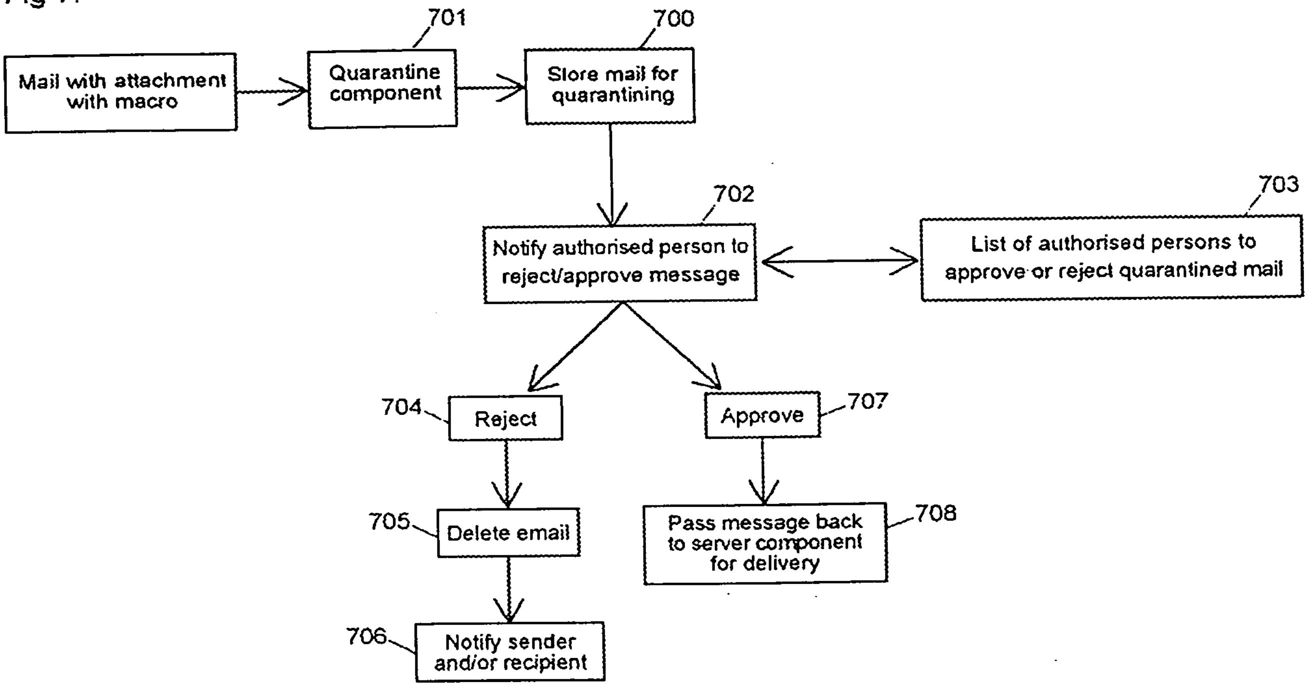

501
Email System
502
Server component
506
Email analyzing component
502
Server component
510
Email
Quarantine Component
701

Fig 7.


Mail with attachment with macro
701
Quarantine component
700
Store mail for quarantining
702
Notify authorised person to reject/approve message
703
List of authorised persons to approve or reject quarantined mail
704
Reject
707
Approve
705
Delete email
708
Pass message back to server component for delivery
706
Notify sender and/or recipient

BLANK PAGE